

# Security Authorization Filter Installation Guide



## Contributors

**Content architect:** Rui Maximo

**Writers:** Rui Maximo

**Editor:** Kelly Fuller Blue

**Published:** January 20, 2017

© MB Corporation 2018. All rights reserved.

This document is the intellectual property of MB Corporation. Neither duplication nor distribution is allowed without written permission of MB Corporation. No distribution outside the customer's organization is allowed.

Security Edge Filter, Security Web Filter, Security Federation Filter, Security Authorization Filter, Security Sync Filter and Security Filter Manager are copyrights of MB Corporation.

All trademarked names in this document are the property of their respective owners.

Security-Filters.com/Lync-Solutions.com operates under the legal entity "MB Corporation", and is incorporated in the State of Washington.

MB Corporation, by publishing this document, does not guarantee that any information contained herein is and will remain accurate or that use of the information will ensure correct and faultless operation of the relevant service or equipment. MB Corporation, its agents and employees shall not be held liable to or through any user for any loss or damage whatsoever results from relying on the information contained herein.

Nothing in this document is intended to and does not alter the legal obligations, responsibilities, or relationship between you and MB Corporation as set out in the contract existing between you and MB Corporation. MB Corporation will not be liable for any compliance or technical information provided herein.

This document is provided "as-is." The information and views expressed in this document, including URL and other Internet website references, may change without notice.

Information in the examples in this document is fictitious and is only for illustration. No actual association or connection is in any way intended or should be inferred.

Table of contents

1 Security Authorization Filter ..... 5

2 Security Concern ..... 5

3 Solution ..... 5

4 Security Authorization Filter ..... 7

4.1 Configure Security Authorization Filter ..... 7

4.2 Install Security Authorization Filter ..... 9

4.3 Monitor Security Authorization Filter ..... 10

4.4 Troubleshooting ..... 10

## 1 Security Authorization Filter

The Security Authorization Filter is a security solution to restrict mobile devices from accessing Skype for Business Server to only authorized devices by the administrator. Authorized devices are strongly mapped to a specific user, and only that user is allowed to connect to your Skype for Business Server environment from the specific device.

## 2 Security Concern

When customers enable Skype for Business Mobile access, their users sign in to your Skype for Business Servers from any device with the Skype for Business Mobile application installed. With a proliferation of mobile devices signed in to your Skype for Business Servers, this puts your network at risk from account high jacking, improper disclosure of confidential information and privacy concerns. The administrator has no ability to control which devices users are permitted to sign-in from, track these devices and block them should they get lost or stolen. Figure 2.1 illustrates mobile devices potentially putting your network at risk because users can sign-in from any device given the correct credentials.

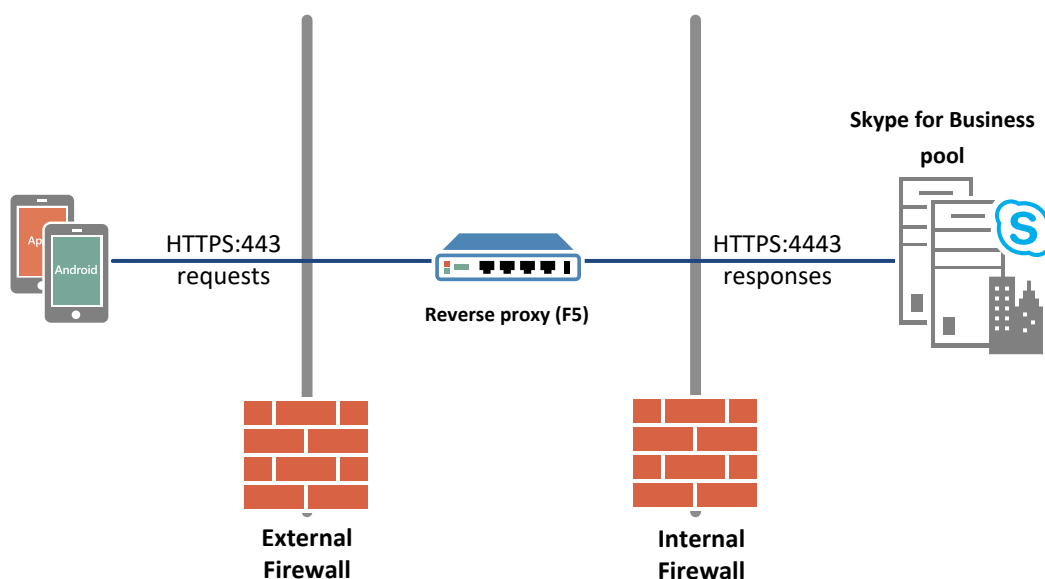


Figure 2.1 Proliferation of Skype for Business Mobile devices that users can sign-in to connecting directly to your infrastructure.

## 3 Solution

The Mobile Protection solution restricts access from mobile clients to connect to your Skype for Business Server infrastructure only if the mobile device has been authorized. If the Skype for Business Mobile client is not authorized, it will have restricted access. If the administrator marks the device as unauthorized, the device will be blocked at the reverse proxy by the Security Web Filter. A Skype for Business Mobile client can be authorized by the administrator or self-registered

by the user (i.e. owner of the mobile device). Once the device is authorized, the mobile client registered to that user and only that user. Should another user attempt to sign-in from the same device, the sign-in request will be blocked. There is a one-to-one mapping between Skype for Business Mobile client and user.

Since a user can be signed in to a Skype for Business Mobile client for up to 8 hours before the user is challenged for credentials again, there's no way to log off the user within that time period. With the Mobile Protection solution, this is now possible. Each sign-in session is tracked on a per device basis, and therefore the Security Web Filter can block the sign-in session when the administrator marks a device as unauthorized.

This solution's architecture consists of the following components:

- Security Authorization Filter
- Security Web Filter
- Security Filter Manager

Figure 3.1 illustrates the architecture of the Mobile Protection solution.

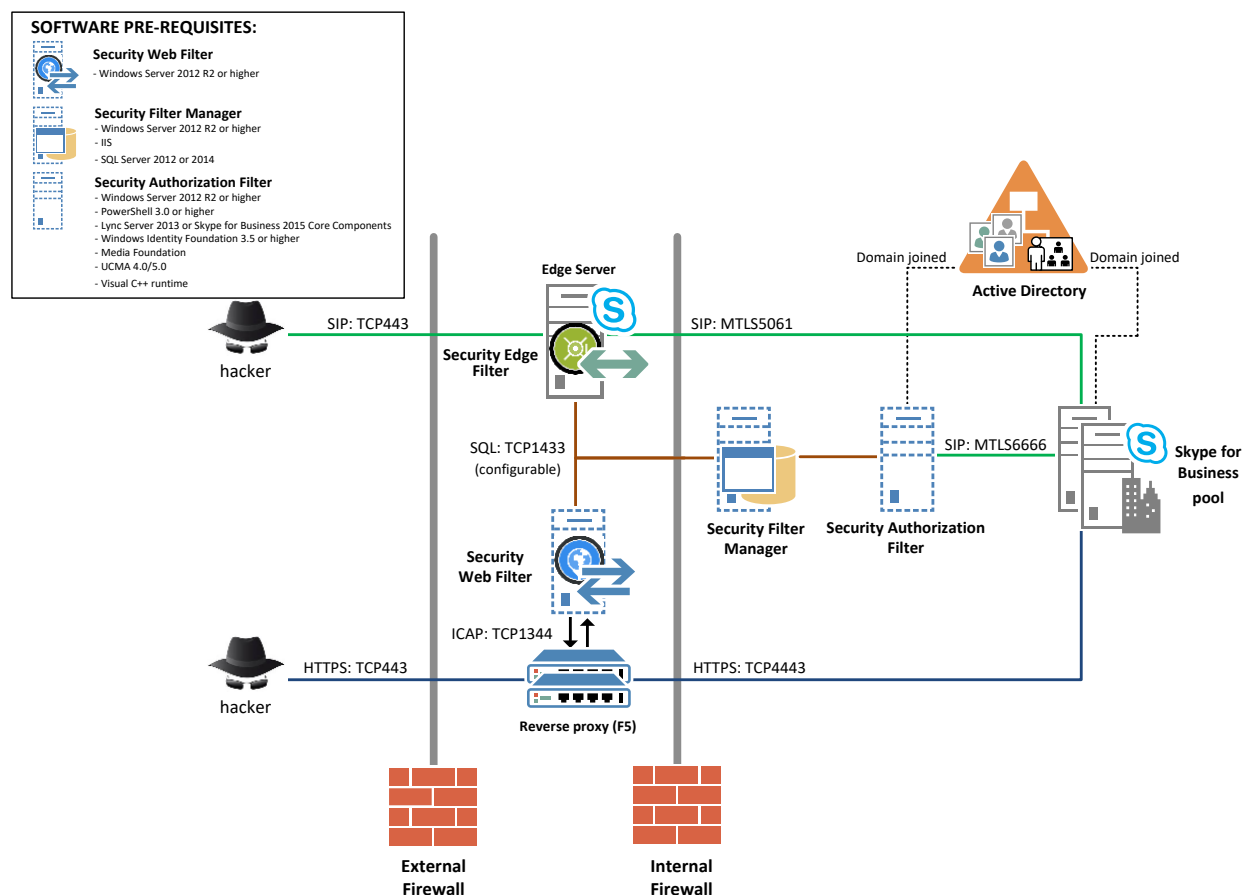


Figure 3.1 Mobile Protection architecture

## 4 Security Authorization Filter

After the Security Filter Manager is installed and configured, you can install the Security Authorization Filter. The Security Authorization Filter prompts the user via IM to enter their authorization code when signing in to Skype for Business Server from a mobile client that has not been authorized before.

The Security Authorization Filter is installed as a service on Windows Server 2012 R2 64-bit or later. This server must be joined to Active Directory. The Windows Firewall on the Security Authorization Filter server must allow TCP traffic on port 1433 (SQL) and port 6666 (SIP). Install the following Windows components on the server where you'll install the Security Authorization Filter:

- .NET Framework 4.5
- PowerShell 3.0 or higher
- Lync Server 2013 or Skype for Business 2015 Core Components
- Windows Identity Foundation 3.5 or higher
- Media Foundation
- Unified Communications Managed API (UCMA) 4.0 or 5.0 runtime with all updates
- Visual C++ runtime (VCRedist\_x64 available on your Lync Server 2013 or Skype for Business 2015 installation media)

Hardware (physical or virtual) requirements:

Hardware component	Recommended
CPU	64-bit dual processor, quad-core, 2.26 gigahertz (GHz) or higher.
Memory	8 gigabytes.
Disk	1 drive (200 GB or more) 10,000 rpm or higher speed
Network	1 dual-port network adapter, 1 Gbps or higher.

### 4.1 Configure Security Authorization Filter

The following configuration steps only need to be run once. Do not run these steps on subsequent installations of the Security Authorization Filter.

You must be logged in as a member of the domain **RTCCUniversalServerAdmins** group and a member of the **local administrator** group.

The Security Authorization Filter must be installed on a server joined to your internal Active Directory Directory Services where your Skype for Business Server infrastructure is deployed. Use the Skype for Business Server 2015 – Deployment Wizard to install the **Local Configuration Store** and assign a **certificate** to this server where the Security Authorization Filter will be installed (Figure 4.1.1).

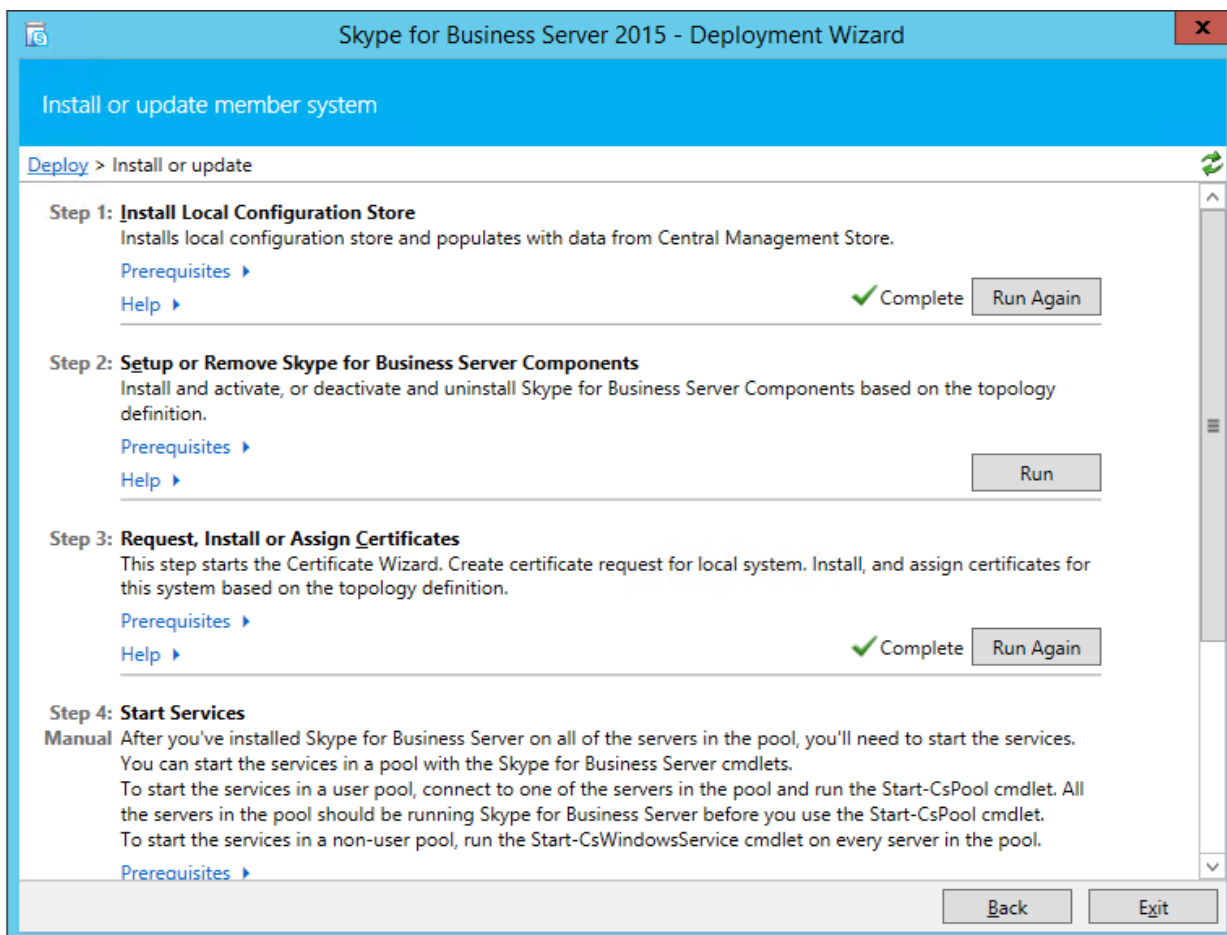


Figure 4.1.1 Skype for Business Server 2015 - Deployment Wizard

Next, configure any Windows firewalls or 3<sup>rd</sup> party firewalls to allow TCP access over SQL port **1433** (default port) between the Security Authorization Filter and the Security Filter Manager, and TCP access over SIP port **6666** between the Security Authorization Filter and your Skype for Business Server pools.

Next, you must run the PowerShell script, *configure.ps1*, after you complete the Security Authorization Filter installation (see section 4.2). This PowerShell script is located in *%programFiles%\MB\Security Authorization Filter* to configure the Security Authorization Filter as a Skype for Business trusted application server. This folder becomes available after you complete the Security Authorization Filter installation. Provide the application endpoint SIP address (i.e. [authorizationfilter@contoso.com](mailto:authorizationfilter@contoso.com)) you specified in the PowerShell script, *configure.ps1*, to your



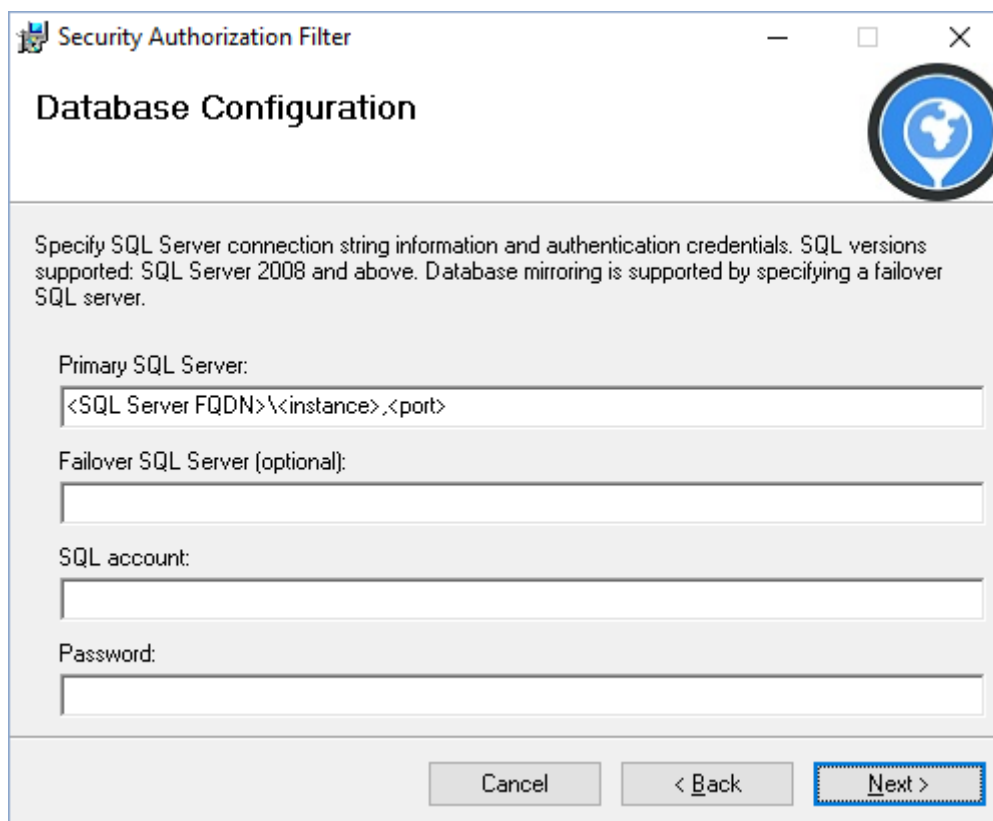
contact at MB Corporation. Alternative, you can retrieve this application endpoint SIP address by running the following PowerShell command: `Get-CSTrustedApplicationEndpoint`. A licensed version of the Security Web Filter will be generated for you.

## 4.2 Install Security Authorization Filter

Before installing the Security Authorization Filter, you must first install and configure the Security Filter Manager. Please refer to the Security Filter Manager Installation Guide for details on how to install.

Here are the installation steps for setting up the Security Authorization Filter.

1. After you download the Security Authorization Filter zip file (that contains `SecurityAuthorizationFilterSetup.msi` and `setup.exe`), run the `setup.exe` with local administrator privileges.
2. The Security Authorization Filter Setup Wizard opens. Click **Next**.
3. On the **License Agreement** page, click **I Agree**, and then click **Next**.
4. Follow the Pre-Requisites instructions. These are the same instructions described in section 4.1. Then click **Next**.
5. On the **Database Configuration** page (see Figure 4.2.1), specify the SQL Server connection string information and the SQL Authentication credentials to connect to the `SecurityFilterManager` database.



The screenshot shows a window titled "Security Authorization Filter" with a "Database Configuration" tab. The window contains a text box for the "Primary SQL Server" with the placeholder text "<SQL Server FQDN>\<instance>,<port>". Below this is a text box for the "Failover SQL Server (optional)". Further down are text boxes for "SQL account:" and "Password:". At the bottom right, there are three buttons: "Cancel", "< Back", and "Next >". The "Next >" button is highlighted with a blue border. A circular logo with a globe is visible in the top right corner of the window.

Figure 4.2.1 SQL Server connection string and SQL Authentication credentials

7. Click **Next**.
8. On the **Confirm Installation** page, click **Next** and then **Close** to complete the installation.
9. Open the **Services** console.
10. Search for the **Security Authorization Filter** service.
11. Change the Security Authorization Filter service account to an account that is a member of the following domain and local groups:
  - a. RTCComponentUniversalServices
  - b. RTCUniversalUserAdmins
  - c. RTC Server Local Group
12. Start the **Security Authorization Filter** service.
13. Verify that it started successfully.

### 4.3 Monitor Security Authorization Filter

The Security Authorization Filter does not store any configuration or data locally. Therefore, there is no need to backup the Security Authorization Filter service. Any events are logged to the Application Event log, and can be viewed in the Event Viewer. When restoring the server, the Security Authorization Filter can be reinstalled or the VM restored to the last snapshot.

### 4.4 Troubleshooting

Before opening a case, please reproduce your issue with verbose logging enabled. This will provide additional information not available in the Application Event Viewer.

To view detailed logging for troubleshooting purposes, open the config file using Notepad or your preferred text editor. Modify the value, "normal", to "verbose" for the key, "logLevel".

```
<add key="logLevel" value="verbose" />
```

Use the DebugView tool to capture this verbose logging. You can download this free tool from [Windows Sysinternals](http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx) (<http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx>).

1. Start Dbgview.exe using administrative privileges, and check the **Capture Global Win32** option as shown in Figure 4.4.1.

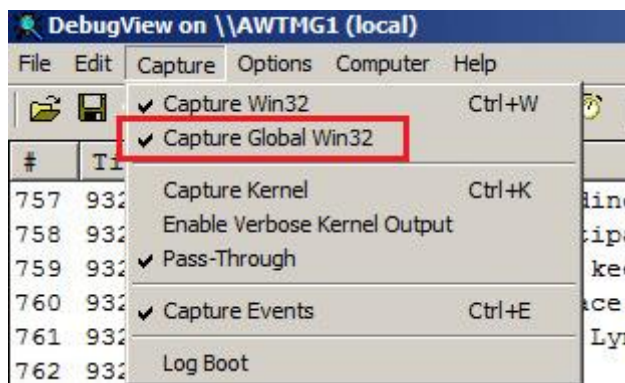


Figure 4.4.1 Options to select for DbgView

2. As soon as you have reproduced the issue, save the output to a text file as shown in Figure 4.4.2.

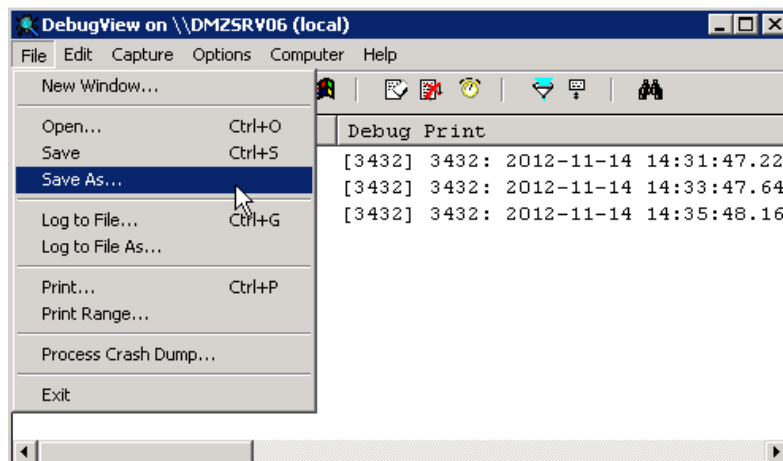


Figure 4.4.2 Debug output